REMARKS

Reconsideration of this application, as amended, is respectfully requested. Claims 1, 2, 5, 10, 19, and 22 have been amended, and support for these amendments may be found throughout the specification as filed, for example at paragraphs 13-15. No new matter is being added.

Claim 1 is directed to statutory subject matter. For example, amended claim 1 recites the injector is stored on a first computing device and redirect code placed by the injector in a memory of the first computing device. The injector in amended claim 1 is tied to a particular machine or hardware, the first computing device, and transforms memory on the first computing device. Thus, the removal of the non-statutory subject matter rejection is respectfully requested.

The specification enables one to make and use the invention as claimed. Without acquiescence to the cited basis for the rejection, independent claims 1, 10, and 22 have been amended. As indicated above, the specification provides support for the amended claims throughout the specification as filed, for example at paragraphs 13-15. For example, claim 1, as amended, recites redirect code placed by the injector in a memory of the first computing device used by an application process, the redirect code allows access to secured data at a remote computer system by authorizing access with security in place at the remote computing system. By way of example, paragraphs [00013-00015] of the present Specification provide examples of embodiments of the claimed invention such as: "firewall 14 may be any hardware and/or software that prevent unauthorized access", "injector agent 26 is preferably a lightweight and transparent piece of application code that is operable to "inject" a piece of redirect code 28 into a communication application 30", "redirect code 28 is operable to enable application 30 to communicate with firewall 14 using its authentication and encryption technology", and "using this technology, users do not have to possess special communication hardware or software to enjoy encrypted communication with firewall to access secured resources 16." Thus, the removal of the failure to comply with the enablement requirement is respectfully requested.

Claim 1 is patentable over Calder et al., US Publication No. 2002/0092003. For example, Calder does not teach or suggest redirect code placed by the injector in a memory of the first

computing device used by an application process, the redirect code allows access to secured data at a remote computer system by authorizing access with security in place at the remote computing system as recited in amended claim 1. Claims 10 and 22 recite similar limitations. Nowhere in Calder is the mention of memory used by an application process with redirect code that authorizes access with security in place at the remote computing system.

In sharp contrast, Calder is directed toward securing an application for execution on an individual computer, and the focus in the cited sections of Calder is on providing additional security to the application to prevent the user of the individual computer from accessing the contents of the application. (Abstract, paragraphs 0077-0078, 0088, and 0092) To that end, Calder teaches encryption of the application to ensure that the user of the individual computer does not improperly access the contents of the application, and transmission of the encrypted application from a server to the individual system (paragraphs 0088 and 0092). Calder does not disclose or suggest memory used by an application process with redirect code that allows access to secured data at a remote computer system, much less memory used by an application process with redirect code that allows access to secured data at a remote computer system by authorizing access with security in place at the remote computing system. Therefore, it follows that claims 1, 10, and 22 (and its dependent claims) are patentable over Calder.

Although not relied upon by the Examiner limitations of claim 1, combining the teachings of Thomas et al., U.S. Patent 6,148,336, with Calder does not alter the above conclusion. Thomas fails to teach or suggest redirect code operable to be placed in a memory of the application process. Specifically, Thomas teaches interception of all network traffic at a lower level than the application. (page 7, lines 32-33) Thus, claims 1, 10, and 22 are patentable over the combination of the cited references, and, hence, all dependent claims are patentable by virtue of their dependency on claims 1, 10, and 22.

For at least the foregoing reasons, the present claims are patentable over the cited references. Please charge our Deposit Account No. 19-3140 for any deficiencies of fees.

Respectfully submitted,
SONNENSCHEIN NATH & ROSENTHAL LLP

Date: December 19, 2008

P.O. Box 061080
Wacker Drive Station
Sears Tower
Chicago, IL 60606-1080
650-798-0320

/Tarek N. Fahmi/
Tarek N. Fahmi
Reg. No. 41,402